WUP.XVA.322.70.ASzu.2020 Szczecin, dn. 3. lipca 2020 r.

ZAPYTANIE OFERTOWE

Postępowanie prowadzone w oparciu o art. 4 pk. 8 ustawy z dnia 29 stycznia 2004 r.
Prawo zamówień publicznych

1. W imieniu Wojewódzkiego Urzędu Pracy w Szczecinie zapraszam do składania ofert na **zapytanie ofertowe** dotyczące:
   Dostawa urządzenia zabezpieczenia brzegu sieci działalacego w Klastrze.
2. Opis przedmiotu zamówienia:

Urządzenie pracujące w klastrze **czyli fizycznie 2 urządzenia które mają się wspierać w razie awarii** ale mogą również pracować oddzielnie. Urządzenia posiadające oprogramowanie wewnętrzne.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów

zabezpieczeń oraz łączy sieciowych.

4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.3 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 2 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 135 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware vCenter (ESXI).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

W celu sumiennego wykonania **osoba wdrażająca musi posiadać** certyfikat NSE8 z proponowanych rozwiązań (certyfikaty załączyć do oferty) oraz aktualne poświadczenie bezpieczeństwa, upoważniające do dostępu do danych o klauzuli min. poufne (certyfikaty załączyć do oferty).

W usługę wliczona musi być konfiguracja wykonana przez Wykonawcę poniższych funkcjonalności w systemie bezpieczeństwa:

1. Interfejsy sieciowe
2. Ustawienia DNS
3. Routing
4. Obiekty
5. Serwisy
6. Harmonogramy
7. Mapowanie adresów
8. Pule IP
9. Kształtowanie ruchu
10. Antywirus
11. Filtrowanie stron www
12. System ochrony przed włamaniem (IPS)
13. Inspekcja SSL
14. Polityki dostępowe
15. VPN
16. Integracja z Active Directory
17. Ustawienie jednokrotnego logowania (SSO)
18. Klaster urządzeń

Konfiguracja odbywać się będzie w filii WUP na ulicy Żubrów 3 w Szczecinie.

3. Nomenklatura wg CPV 35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.
4. Projekt umowy wraz z określeniem warunków zmian umowy stanowi załącznik nr 2 do niniejszego zapytania ofertowego.
5. Wykonawca związany jest ofertą 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
6. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów: Wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy mogą przekazywać drogą elektroniczną (skan dokumentów) na adres przetargi@wup.pl. Wykonawcy sporządzają ofertę ściśle według wymagań określonych w niniejszym zapytaniu ofertowym. Oferta oraz pozostałe dokumenty, dla których Zamawiający określił wzory, winny być sporządzane zgodnie z tymi wzorami. Dokumenty tworzące ofertę muszą być podpisane przez osoby upoważnione do reprezentowania Wykonawcy. Pełnomocnictwo do ich podpisania musi być dołączone do oferty, o ile nie wynika ono z innych dokumentów załączonych przez Wykonawcę. Pełnomocnictwo składane do oferty winno być podpisane przez osoby upoważnione do reprezentowania Wykonawcy. Każdy Wykonawca może złożyć tylko jedną ofertę cenową. Złożenie więcej niż jednej oferty lub alternatywy zawarte w treści oferty spowodują odrzucenie wszystkich ofert, złożonych przez Wykonawcę. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

7. Osoby uprawnione do porozumiewania się z Wykonawcami:
   Pani Anna Szuman lub osoba zastępująca, e-mail: przetargi@wup.pl
8. Warunki udziału w postępowaniu oraz sposób dokonywania oceny ich spełnienia – nie dotyczy.
9. Kryteria oceny ofert – informacja o wagach punktowych lub procentowych przypisanych do poszczególnych kryteriów, opis sposobu przyznawania punktacji:

Kryterium cena: waga – 100 %

Oferta z najniższą zaoferowaną ceną za wykonanie całego przedmiotu zamówienia otrzyma 100 pkt.

Pozostałe oferty otrzymają punkty zgodnie z wyliczeniem wg wzoru:

Wartość punktowa = 100 x (Cmin/Cb)

gdzie:

Cmin - najniższa cena spośród złożonych ofert,

Cb - cena oferty badanej.

Maksymalna liczba punktów, która może zostać przyznana Wykonawcy w ocenie ww. kryterium wynosi 100 pkt.

Punkty zostaną zaokrąglone do dwóch miejsc po przecinku - zgodnie z zasadami matematycznymi.

10. **Cel i przedmiot udostępnianych danych osobowych**

a) Administratorem danych osobowych w zakresie przedmiotowego zamówienia jest Zamawiający – w odniesieniu do danych osobowych osoby/osób wskazanych.
b) Administrator danych odpowiada we własnym zakresie za zapewnienie zgodności ich przetwarzania z przepisami o ochronie danych osobowych.
c) Zarówno Zamawiający jak i Wykonawca zobowiązują się do przetwarzania danych osobowych zgodnie z treścią niniejszego Zapytania ofertowego, Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zw. dalej RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018 poz. 1000, z późn. zm.) a także innych powszechnie obowiązujących przepisach prawa, w celu prawidłowego wykonania przedmiotu zamówienia.
d) W Wojewódzkim Urzędzie Pracy w Szczecinie został powołany Inspektor ochrony danych osobowych, z którym można się skontaktować poprzez adres e-mail: iod@wup.pl lub pisemnie na adres Administratora.
e) Dane osobowe osób wskazanych do kontaktu między Stronami oraz udostępnione przez Wykonawcę dane osobowe osób do realizacji zamówienia przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu realizacji przedmiotu zamówienia.
f) Odbiorcami zgromadzonych danych osobowych osób wskazanych podczas realizacji zamówienia będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w tym Zlecenie wykonania usługi. Dane mogą być przekazane także kurierom oraz podmiotom świadczącym usługi pocztowe oraz na stronie Biuletynu Informacji Publicznej Urzędu.

g) Wykonawca oraz Zamawiający przetwarza dane osobowe zgodnie z obowiązującymi przepisami w zakresie niezbędnym do realizacji niniejszego zamówienia oraz celów podatkowych, rachunkowych i przez czas niezbędny do rozliczenia przedmiotowego zamówienia.

h) Dane osobowe będą przechowywane u Zamawiającego przez okres wynikający z obowiązującego Jednolitego Rzeczowego Wykazu Akt.

i) Obowiązek podania przez Wykonawcę danych osobowych dotyczących bezpośrednio gromadzonych danych osobowych jest wymogiem, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego oraz realizacją przedmiotowego zamówienia.

j) W odniesieniu do zgromadzonych danych osobowych osób wskazanych w trakcie prowadzonego postępowania oraz udostępnionych przez Wykonawcę danych osobowych osób do realizacji zamówienia, decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;

- na podstawie art. 15 RODO, osoba której dane dotyczą posiada prawo dostępu do swoich danych osobowych,
- na podstawie art. 16 RODO, osoba której dane dotyczą posiada prawo do sprostowania swoich danych osobowych,
- na podstawie art. 18 RODO, osoba której dane dotyczą posiada prawo do żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych danej osoby narusza przepisy RODO.

k) W odniesieniu do zgromadzonych danych osobowych osób, osoby której dane dotyczą, nie przysługuje:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania zgromadzonych danych osobowych jest art. 6 ust. 1 lit. c RODO.

l) Gromadzone dane są przez Strony odpowiednio zabezpieczone oraz chronione z zastosowaniem środków technicznych i organizacyjnych, aby dane zgromadzone nie były zmieniane przez osoby nieupoważnione lub nie były udostępniane osobom nieupoważnionym.

11. Formularz oferty cenowej:

a) Na załączonym formularzu cenowo-ofertowym, należy przedstawić kwotę brutto za wykonanie przedmiotu zamówienia.

b) Wartość cenową należy podać w złotych polskich cyfrą – z dokładnością do dwóch miejsc po przecinku oraz słownie.

c) Cena powinna zawierać wszelkie koszty związane z wykonaniem przedmiotu zamówienia.

d) Wszelkie rozliczenia pomiędzy Zamawiającym a Wykonawcą odbywać się będą w złotych

polskich.

12. Informacje o formalnościach:

a) Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający zawiadomi wszystkich Wykonawców, którzy ubiegali się o udzielenie zamówienia o wyniku postępowania.

b) Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną ofertę najkorzystniejszą spośród złożonych ofert, bez przeprowadzania ich ponownej oceny.

c) Niniejsze postępowania prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach organizacyjnych Zamawiającego. Nie mają w tym przypadku zastosowania przepisy Ustawy Prawo zamówień publicznych.

d) Zamawiający poprawia w ofercie:

I. oczywiste omyłki pisarskie,

II. oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,

III. inne omyłki polegające na niezgodności oferty z treścią zapytania ofertowego, niepowodujące istotnych zmian w treści oferty

– niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

e) Zamawiający zastrzega sobie prawo do unieważnienia przedmiotowego postępowania na każdym etapie trwania, bez podania przyczyny.

13. Dokumenty, jakie Wykonawca powinien załączyć do oferty:

a) wypełniony i podpisany Formularz cenowo-ofertowy – wg. załączonego wzoru

b) certyfikat NSE8 z proponowanych rozwiązań osoby wdrażającej **oraz** aktualne poświadczenie bezpieczeństwa, upoważniające do dostępu do danych o klauzuli min. Poufne.

c) jeżeli z przedstawionych dokumentów wynika, że osoba, która podpisała ofertę nie jest uprawiona do reprezentacji Wykonawcy w obrocie gospodarczym, do oferty załączyć należy dokument pełnomocnictwa; w przypadku złożenia kopii pełnomocnictwa musi być ono potwierdzone za zgodność z oryginałem przez wykonawcę.

d) w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania **dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski**, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) **oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością** tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

e) oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

W przypadku nie złożenia wraz z ofertą wymaganego pełnomocnictwa i/lub wymaganych certyfikatów/poświadczeń Zamawiający uprawniony jest do żądania od Wykonawcy ich uzupełnienia oraz żądania składania wszelkich wyjaśnień w zakresie związanym z prowadzonym postępowaniem. **Wezwanie do uzupełnienia brakujących/błędnych dokumentów nastąpi tylko raz.**

14. Miejsce składania ofert

Ofertę cenową należy przesłać drogą elektroniczną na adres e-mail przetargi@wup.pl **w terminie do dnia 13 lipca 2020 r. , godz. 12:00.**

Załączniki:

1. Formularz cenowo-ofertowy
2. Projekt umowy wraz z określeniem warunków zmian umowy

ZATWIERDZIŁ:

03. LIP. 2020

DYREKTOR
Wojewódzkiego Urzędu Pracy
.....
Andrzej Przewoda

Data i podpis Kierownika Zamawiającego

Wojewódzki Urząd Pracy
ul. Mickiewicza 41
70-383 Szczecin

WUP.XVA.322.70.ASzu.2020
(znak sprawy)

....., dn. .....

.....

(pieczęć adresowa Wykonawcy)

NIP: .....
REGON:.....
tel.: .....
fax: .....
E-MAIL: .....

FORMULARZ CENOWO-OFERTOWY

W odpowiedzi na zapytanie ofertowe prowadzone w oparciu o art. 4 pkt 8 Ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych na:

Dostawa urządzenia zabezpieczenia brzegu sieci działającego w Klastrze.

Nazwa nadana zamówieniu.

Ja/My, niżej podpisany/i,

.....

działając w imieniu i na rzecz:

.....

1. **Oferujemy wykonanie przedmiotu zamówienia za kwotę:** Brutto: _____zł
2. Przedmiot zamówienia wykonamy w terminie do 14 dni kalendarzowych.
3. Oświadczamy, iż uważamy się za związanych niniejszą ofertą przed okres 30 dni licząc od daty wyznaczonej na składanie ofert.
4. Oświadczamy, że zapoznaliśmy się z postanowieniami zawartymi w projekcie umowy i zobowiązujemy się, w przypadku wyboru naszej oferty jako najkorzystniejszej, do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.
5. **Oświadczam(y), że** wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.*

.....
miejscowość i data

.....
/Podpis i pieczęć osoby upoważnionej do podpisywania oferty/

1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

Umowa nr WUP/...../20120

zawarta w dniu .... r.

dotyczy postępowania WUP.XVA.332.70.ASzu.2020

pomiędzy:

Województwem Zachodniopomorskim - Wojewódzkim Urzędem Pracy w Szczecinie,
przy ul. A. Mickiewicza 41, reprezentowanym przez:
.....
a
.....
zwanym dalej **„Wykonawcą"** o następującej treści:

niniejsza umowa zostaje zawarta z wybranym Wykonawcą na podstawie art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (tekst jednolity Dz. U. z 2019 r. poz. 1843) zwanej w dalszej części umowy **„Ustawą"**

§ 1

1. Wykonawca zobowiązuje się wykonać przedmiot umowy zgodnie z opisem przedmiotu zamówienia stanowiącym Załącznik nr 1 do umowy, zgodnie z zasadami współczesnej wiedzy technicznej oraz obowiązującymi przepisami i normami w ramach postępowania o udzielenie zamówienia publicznego pod nazwą: **Dostawa urządzenia zabezpieczenia brzegu sieci działającego w Kłastrze** a Zamawiający zobowiązuje się do dokonania zapłaty w wysokości określonej w ofercie cenowej stanowiącej Załącznik nr 2 do umowy.
2. Łączna cena przedmiotu zamówienia wynosi ..... **netto,** co stanowi wartość ..... **zł brutto (sł. .....),** zgodnie z Formularzem cenowo-ofertowym stanowiącym Załącznik nr 2 do niniejszej umowy.
3. Za wykonanie przedmiotu umowy określonego w § 1 ust. 1 niniejszej umowy Wykonawca wystawi na podstawie protokołu odbioru, o którym mowa w § 2, fakturę VAT w kwocie brutto przy uwzględnieniu wartości jednostkowych wskazanych w Załączniku nr 2 do niniejszej umowy.
4. Zapłata należności za wykonanie przedmiotu zamówienia nastąpi przelewem przez Zamawiającego, na konto Wykonawcy wskazane w fakturze VAT, w terminie do 14 dni od daty otrzymania prawidłowo sporządzonej faktury. Podstawą do wystawienia faktury jest dokonanie odbioru zgodnie z § 2 ust. 1 umowy
5. Za datę zapłaty należności uważa się dzień obciążenia rachunku bankowego Zamawiającego.
7. Przedstawicielem Zamawiającego w zakresie spraw związanych z realizacją niniejszej umowy jest **Pan Piotr Rzetecki**, adres e-mail: piotr_rzetecki@wup.pl lub **Pan Michał Potrzebny**, adres e-mail: michal_potrzebny@wup.pl.

8. Przedstawicielem Wykonawcy w zakresie spraw związanych z realizacją niniejszej umowy jest ..... adres e-mail: .....
9. Osoba wdrażająca wskazana w ust. 8 posiada certyfikat NSE8 z proponowanych rozwiązań oraz aktualne poświadczenie bezpieczeństwa, upoważniające do dostępu do danych o klauzuli min. Poufne, które stanowią Załącznik nr 3 do niniejszej umowy.

§ 2

1. Dokumentem potwierdzającym wykonanie usługi określonej w § 1 ust. 1 niniejszej umowy będzie sporządzony przez Zamawiającego i podpisany przez Strony protokół odbioru, po wykonaniu przedmiotu zamówienia określonego w Załączniku nr 1 do niniejszej umowy.

§ 3

1. Zamawiający zastrzega sobie prawo potrącenia kar umownych z tytułu niewykonania lub nienależytego wykonania umowy w wysokości 20% należnego wynagrodzenia wynikającego z umowy, z wynagrodzenia należnego Wykonawcy.
2. W przypadku opóźnienia w realizacji przedmiotu zamówienia Zamawiający potrąci karę umowną w wysokości 0,5% za każdy dzień opóźnienia w tryble wskazanym w § 3 ust. 1 niniejszej umowy.
3. W przypadku, gdy kary umowne przewidziane w § 3 ust. 1 niniejszej umowy nie pokryją w całości powstałej szkody, Zamawiający ma prawo dochodzić odszkodowania do pełnej wysokości.
4. W przypadku naruszenia postanowień zawartej umowy, Zamawiający może odstąpić od umowy ze skutkiem natychmiastowym, z zachowaniem prawa do kary umownej określonej w § 3 ust. 1 umowy.

§ 4

1. Wykonawca oświadcza, że przedmiot zamówienia, o którym mowa w § 1 jest wolny od wad prawnych, którego końcowym użytkownikiem będzie Zamawiający.
2. Strony ustalają, że gdyby okazało się, iż osoba trzecia składa roszczenia pod adresem przedmiotu zamówienia, Wykonawca po zawiadomieniu przez Zamawiającego nie uchyli się od niezwłocznego przystąpienia do wyjaśnienia sprawy oraz wystąpi przeciwko takim roszczeniom na własny koszt i ryzyko a nadto, że zaspokoi wszelkie uzasadnione roszczenia, a w razie ich zasądzenia od Zamawiającego regresowo zwróci Zamawiającemu całość uiszczonych, wydatków w tym wydatków i opłat obejmujących koszty procesu i obsługi prawnej.
3. Jeśli przedmiot zamówienia zawierać będzie wady fizyczne uniemożliwiające korzystanie z przedmiotu zamówienia i przysługujących Zamawiającemu praw, Wykonawca zobowiązany jest do dostarczenia w wyznaczonym przez Zamawiającego terminie przedmiotu zamówienia wolnego od wad, chyba, że z przyczyn obiektywnych nie jest w stanie tego wykonać. W przypadku niedostarczenia przedmiotu zamówienia wolnego od wad, bez względu na przyczyny, Zamawiający odstąpi od Umowy ze skutkiem wynikającym z § 3 ust. 1.
4. Wykonawca zobowiązuje się, że wykonując Umowę nie naruszy praw majątkowych osób trzecich, a dostarczony przedmiot umowy nie będzie obciążony prawami osób trzecich w takim zakresie, że kolidowałoby to z wykonaniem Umowy.

§ 5

1. Przedmiot umowy zostanie zrealizowany w terminie **do 14 dni kalendarzowych** od dnia zawarcia umowy, zgodnie z opisem przedmiotu zamówienia stanowiącym Załącznik nr 1 do niniejszej umowy.

§ 6

1. Zamawiający może odstąpić od umowy w razie istotnych zmian okoliczności powodujących, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy.
2. Zamawiający może również odstąpić od umowy w przypadku naruszenia przez Wykonawcę istotnych postanowień niniejszej umowy, po uprzednim wezwaniu do zaprzestania naruszania w zakreślonym terminie z zagrożeniem odstąpienia od umowy w tym trybie.

§ 7

1. Strony zobowiązują się interpretować postanowienia niniejszej umowy w sposób zmierzający do zapewnienia partnerskiej współpracy między nimi.
2. Spory powstałe w związku z niniejszą umową będą rozstrzygane przez Strony przede wszystkim na drodze polubownej.
3. Jeżeli strony nie osiągną kompromisu na drodze polubownej, sprawy sporne rozpoznawane będą przez Sąd powszechny właściwy dla siedziby Zamawiającego. Przed wniesieniem powództwa, każda ze stron obowiązana jest co najmniej wezwać listem poleconym drugą Stronę do próby ugodowego zakończenia sporu.
4. W sprawach nieuregulowanych niniejszą umową będą miały zastosowanie przepisy Kodeksu Cywilnego.

§ 8

1. Strony zobowiązują się do informowania o wszelkich zmianach danych stron umowy, które mogą mieć wpływ na realizację niniejszej umowy.
2. Ewentualne spory, które mogą wyniknąć na tle wykonania postanowień umowy strony podejmą się rozstrzygnąć polubownie. W razie braku możliwości polubownego rozwiązania sporów, będą one rozstrzygane przez właściwy rzeczowo Sąd w Szczecinie.
3. Niniejsza umowa wchodzi w życie z dniem jej podpisania przez obie strony.
4. Załączniki do niniejszej umowy stanowią jej integralną część.
5. Wykonawca oświadcza, iż pozyskując i przetwarzając dane osobowe wypełnił obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu ubiegania się o udzielenie zamówienia publicznego oraz jego realizację.

6. Wykonawca zobowiązuje się zachować w tajemnicy wszelkie informacje uzyskane w związku z realizacją przedmiotu umowy i nie udostępniać ich w jakiejkolwiek formie osobom trzecim, tak w czasie trwania umowy, jak i po jej zakończeniu czy rozwiązaniu.
7. Strony dopuszczają ujawnienie informacji jedynie pracownikom Stron, w zakresie niezbędnym do wykonania umowy, zapewniając przy tym, aby podmioty te nie ujawniały informacji osobom trzecim zgodnie z § 9 ust. 6 umowy.
8. Wymogi zawarte w § 9 ust. 6 i 7 nie będą miały zastosowania do tych informacji, które:
   1) są opublikowane, powszechnie znane lub urzędowo podane do publicznej wiadomości;
   2) zostaną ujawnione przez jedną ze Stron za uprzednią pisemną zgodą drugiej Strony;
   3) zostaną ujawnione przez Strony na żądanie organu sądowego lub administracyjnego, albo gdy obowiązek ujawnienia wynika z bezwzględnie obowiązujących przepisów prawa.
9. W takim wypadku Wykonawca zobowiązuje się bezzwłocznie poinformować drugą Stronę o fakcie ujawnienia.
10. Obowiązek określony w § 9 ust. 6-8 niniejszej umowy nie uchybia obowiązkom Stron wynikającym z przepisów prawa powszechnie obowiązującego w zakresie ochrony danych osobowych, w szczególności wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zw. dalej RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018 poz. 1000, z późn. zm.).
11. Wykonawca zobowiązuje się do podjęcia wszelkich niezbędnych kroków mających na celu zapewnienie, że żadna z osób skierowanych do realizacji przedmiotu zamówienia, otrzymujących informacje, nie ujawni tych informacji ani ich źródła w całości, jaki i w części osobom trzecim bez wyraźnego pisemnego upoważnienia Zamawiającego.
12. Wykonawca zobowiązuje się nie kopiować, nie powielać ani w jakikolwiek sposób rozpowszechniać jakichkolwiek informacji, z wyjątkiem przypadków, w jakich jest to konieczne w celach realizacji niniejszej umowy. W powyższych przypadkach wszelkie kopie lub reprodukcje będą własnością Zamawiającego.
13. Administratorem[1]* w zakresie przedmiotowej umowy jest Wojewódzki Urząd Pracy w Szczecinie, mający siedzibę przy ul. Mickiewicza 41, 70-383 Szczecin. Z administratorem danych można się skontaktować poprzez adres e-mail: sekretariat@wup.pl lub telefonicznie pod numerem 91/42-56-102 lub pisemnie na adres siedziby administratora.
14. W Wojewódzkim Urzędzie Pracy w Szczecinie został powołany Inspektor ochrony danych osobowych, z którym można się skontaktować poprzez adres e-mail: iod@wup.pl lub pisemnie, na w/w adres administratora.

---

[1] Administrator – Zgodnie z art. 4 pkt 7 RODO to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. W niniejszej Polityce ochrony danych przez Administratora rozumie się Dyrektora Wojewódzkiego Urzędu Pracy w Szczecinie

15. Dane osobowe zgromadzone w ramach przedmiotowej umowy przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu realizacji przedmiotowej umowy.
16. Odbiorcami zgromadzonych danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w tym przedmiotowa umowa. Dane mogą być przekazane także kurierom oraz podmiotom świadczącym usługi pocztowe oraz na stronie Biuletynu Informacji Publicznej Urzędu.
17. Dane osobowe będą przechowywane przez okres wynikający z Jednolitego Rzeczowego Wykazu Akt obowiązującego u Zamawiającego.
18. Obowiązek podania przez Wykonawcę danych osobowych dotyczących bezpośrednio gromadzonych danych osobowych jest wymogiem, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego oraz realizacją przedmiotowej umowy.
19. W odniesieniu do zgromadzonych danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
    a) na podstawie art. 15 RODO, osoba której dane dotyczą posiada prawo dostępu do swoich danych osobowych,
    b) na podstawie art. 16 RODO, osoba której dane dotyczą posiada prawo do sprostowania swoich danych osobowych,
    c) na podstawie art. 18 RODO, osoba której dane dotyczą posiada prawo do żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,
    d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych danej osoby narusza przepisy RODO.
20. W odniesieniu do zgromadzonych danych osobowych, osobie której dane dotyczą, nie przysługuje:
    a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
    b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
    c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania zgromadzonych danych osobowych jest art. 6 ust. 1 lit. c RODO.
21. Gromadzone dane są odpowiednio zabezpieczone oraz chronione z zastosowaniem środków technicznych i organizacyjnych, aby dane zgromadzone nie były zmieniane przez osoby nieupoważnione lub nie były udostępniane osobom nieupoważnionym.

§ 9

Umowę sporządzono w 2 jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

Załącznik:

1. Opis przedmiotu zamówienia.
2. Formularz cenowo-ofertowy.
3. Certyfikat NSE8 z proponowanych rozwiązań oraz aktualne poświadczenie bezpieczeństwa.
4. Umowa powierzenia danych.

.....
Zamawiający

.....
Wykonawca

RADCA PRAWNY
Wojewódzkiego Urzędu Pracy
Błażej Wasilewski

Umowa powierzania danych

NR UMOWY: ...../.....

zawarta w dniu .....

dotycząca postepowania WUP.XVA.322.70.ASzu.2020

będąca załącznikiem do umowy WUP/...../2020

pomiędzy:

Województwem Zachodniopomorskim - Wojewódzkim Urzędem Pracy w Szczecinie, ul. A. Mickiewicza 41, 70-383 Szczecin, reprezentowanym przez:

Pana Andrzeja Przewodę – Dyrektora Wojewódzkiego Urzędu Pracy w Szczecinie

zwanym dalej **„Administratorem danych lub Administratorem"**,

a

.....,

zwanym dalej **„Podmiotem przetwarzającym"**

o następującej treści:

§ 1.

Definicje

1. **Dane osobowe** –oznacza to dane osobowe w rozumieniu Rozporządzenia Parlamentu Europejskiego i Radny (UE) 2016/679, 679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. **Administrator danych osobowych** – Wojewódzki Urząd Pracy reprezentowany przez Dyrektora Wojewódzkiego Urzędu Pracy;
3. **Podmiot przetwarzający** – .....
4. **Przetwarzanie danych osobowych"** oznacza to przetwarzanie w rozumieniu art. 4 pkt 2 RODO, tj. operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
5. **Naruszenie ochrony danych osobowych** – zgodnie z definicją zawartą w art. 4 pkt 12 RODO, naruszenie ochrony danych osobowych oznacza incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem: zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych;
6. **RODO**- Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

§2

Zakres i cel przetwarzania danych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w tryble art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „RODO" oraz zgodnie z przepisem art. 31 Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000 ze zm.) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia RODO.
4. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu *realizacji umowy z dnia ..... nr WUP/..../2020 w zakresie dostawy urządzenia zabezpieczenia brzegu sieci działającego w Klastrze oraz jego wdrożenia.*
5. *Przetwarzanie dotyczy następujących kategorii danych: (imię, nazwisko, adres e-mail, login).*
6. *Dane będą przetwarzane w formie elektronicznej.* [1]
7. Podstawą przetwarzanie danych osobowych o których mowa w pkt 5 jest art. 6 ust. 1 lit. c
8. Powierzeniu podlegają dane zwykłe.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. Przy przetwarzaniu danych osobowych podmiot przetwarzający zobowiązuje się do przestrzegania zasad wskazanych w niniejszym paragrafie, w ustawie o ochronie danych osobowych, RODO oraz innych przepisach prawa powszechnie obowiązującego dotyczącego ochrony danych osobowych.
4. Podmiot przetwarzający informuje Administratora:

[1] Niepotrzebne skreślić

a/ W ciągu 24 godzin od stwierdzenia naruszenia o wszelkich przypadkach naruszenia ochrony danych osobowych lub o ich niewłaściwym użyciu oraz naruszeniu obowiązków dotyczących ochrony powierzonych do przetwarzania danych osobowych. Zgłoszenie powinno oprócz elementów określonych w art. 33 ust. 3 RODO zawierać informacje umożliwiające Administratorowi danych określenie czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. Jeżeli informacji, o których mowa w art. 33 ust. 3 RODO nie da się udzielić w tym samym czasie, podmiot przetwarzający może je udzielać sukcesywnie bez zbędnej zwłoki. Zgłoszenie należy wysłać na adres mailowy: iod@wup.pl.

b/ niezwłocznie o wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych prowadzonych w szczególności przed Prezesem Urzędu Ochrony Danych Osobowych, Europejskim Inspektorem Ochrony danych Osobowych, urzędami państwowymi, policją lub przed sądem;

c/ niezwłocznie o wynikach kontroli prowadzonych przez podmioty uprawnione w zakresie przetwarzania danych osobowych wraz z informacją na temat zastosowania się do wydanych zaleceń.

5. Podmiot przetwarzający zobowiązuje się do udzielenia Administratorowi, na każde żądanie, informacji na temat przetwarzania danych osobowych, o których mowa w niniejszym paragrafie, a w szczególności niezwłocznego przekazywania informacji o każdym przypadku naruszenia obowiązków dotyczących ochrony danych osobowych.
6. Podmiot przetwarzający pomaga wywiązać się z Administratorowi z obowiązków określonych w art. 32 - 36 RODO.
7. Podmiot przetwarzający pomaga Administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.

§4
Prawo kontroli

1. Podmiot przetwarzający zobowiązany jest umożliwić Administratorowi danych osobowych lub podmiotowi przez niego upoważnionemu, dokonanie kontroli zgodności z ustawą, Rozporządzeniem RODO przetwarzania powierzonych danych osobowych w związku z realizacją umowy nr...../.....w miejscach, w których są one przetwarzane. Zawiadomienie o zamiarze przeprowadzenia kontroli zostanie przekazane podmiotowi przetwarzającemu co najmniej 5 dni roboczych (tj. liczonych od poniedziałku do piątku) przed rozpoczęciem kontroli.
2. Podmiot przetwarzający zobowiązany jest umożliwić Administratorowi danych osobowych lub podmiotowi przez niego upoważnionemu, także dokonanie niezapowiedzianej kontroli w przypadku powzięcia wiadomości o rażącym naruszeniu zobowiązań wynikających z ustawy, Rozporządzenia lub niniejszej Umowy.
3. Podmiot przetwarzający zobowiązany jest zastosować się w terminie wskazanym przez Administratora lub podmiot przez niego upoważniony, do zaleceń dotyczących poprawy jakości

zabezpieczenia powierzonych do przetwarzania danych osobowych oraz sposobu ich przetwarzania, sporządzonych w wyniku kontroli przeprowadzonych przez Administratora danych osobowych lub podmiot przez niego upoważniony.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może udostępniać i podpowierzać innym podmiotom powierzone dane pod warunkiem uzyskania uprzedniej i pisemnej zgody Administratora danych oraz kiedy podpisanie umowy podpowierzenia jest niezbędne w celu wykonania umowy.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 pkt 1. Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
5. W sytuacji wskazanej w ust. 1 Wykonawca ma obowiązek zobowiązania swojego podwykonawcy do zachowania zasad i wprowadzenia procedur bezpieczeństwa wobec przekazanych lub powierzonych mu do przetwarzania danych osobowych w zakresie nie mniejszym niż określone w niniejszej umowie.

§ 6

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *określony* od ..... do..... (z uwzględnieniem* **§8 pkt. 3)**
2. Administrator może wypowiedzieć niniejszą Umowę z zachowaniem ..... * okresu wypowiedzenia.

§ 7

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

2. **Rozwiązanie umowy powierzenia jest równoznaczne z rozwiązaniem umowy głównej.**

§ 8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Podmiot przetwarzający zobowiązuje się usunąć w sposób trwały i nieodwracalny wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych pozyskane w związku z realizacją zadań wynikających z realizacji umowy, niezwłocznie, co zostanie potwierdzone stosownym oświadczeniem przekazanym do Administratora danych.

§9

Odpowiedzialność

1. W przypadku nałożenia na Administratora danych osobowych prawomocnej administracyjnej kary pieniężnej na podstawie art. 83 Rozporządzenia lub zasądzenia prawomocnego odszkodowania, o którym mowa w art. 82 Rozporządzenia, w związku z niezgodnym z prawem przetwarzaniem danych osobowych przez Podmiot przetwarzający, Podmiot przetwarzający zapłaci karę umowną w wysokości 100% administracyjnej kary pieniężnej lub odszkodowań nałożonych na Administratora.
2. Podmiot przetwarzający odpowiada za szkody majątkowe lub niemajątkowe, jakie powstały wobec osób trzecich w wyniku przetwarzania danych przez Zleceniodawcę naruszającego Rozporządzenie lub inne przepisy dotyczące ochrony danych osobowych.
3.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.

2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla Administratora danych

....

Administrator danych osobowych Wojewódzki Urząd Pracy w Szczecinie Podmiot przetwarzający -czytelny podpis